

IN THE UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

MICHAL JERZY PIOTROWICZ,

Defendant.

**UNDER SEAL**

Case No. 1:20-mj-201

**AFFIDAVIT IN SUPPORT OF A  
CRIMINAL COMPLAINT AND ARREST WARRANT**

I, Raymond Abruzzese, being duly sworn, depose and state:

1. I am a Special Agent with the U.S. Department of Homeland Security (“DHS”), Homeland Security Investigations (“HSI”), and have been by employed by HSI since 2003. I am currently assigned to the Office of HSI, Washington, D.C. (“HSI DC”), and have investigated crimes relating to child exploitation on the internet since approximately October 2016.

2. I have advanced and on-the-job training in child exploitation on the internet and have participated in federal, multi-jurisdictional, and international investigations, many of which involved child exploitation and/or child pornography offenses. As part of my current duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal distribution, receipt, transportation, possession, and access with intent to view child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A(a). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256).

3. This affidavit is submitted in support of a criminal complaint and arrest warrant for Michal Jerzy Piotrowicz (“PIOTROWICZ”) for a violation of Title 18, United States Code, Section 2252(a)(2), which makes it a crime to knowingly receive child pornography.

4. I am familiar with the information contained in this affidavit based upon the investigation that I have conducted, along with my conversations with other law enforcement officers, computer forensic agents and others, and my review of reports and database records.

5. This affidavit is submitted for the limited purpose of obtaining a criminal complaint and arrest warrant. It does not include each and every fact known to me or the government about the investigation. I have set forth only those facts that I believe are necessary to establish probable cause.

**BACKGROUND FOR PEER-TO-PEER FILE SHARING,  
BITTORRENT NETWORK**

6. Peer-to-peer (“P2P”) file sharing is a method of communication available to internet users through the use of software downloaded from the internet. It is used to share digital files between different users of a P2P network. The hallmark of P2P file sharing is that users of a particular P2P network upload and download files to and from one another’s computers, as opposed to a centralized server. As a result, the availability of a particular file on a P2P network at any given time depends on whether any other users are connected to the network and making that file available.

7. The BitTorrent network is one of several P2P file-sharing networks on the internet. It can be accessed by computers running many different client programs. These programs share common protocols for network access and file sharing. The user interface, features and configuration may vary between clients and versions of the same client.

8. Examples P2P clients, or file sharing applications, on the BitTorrent network include uTorrent and LimeWire. Both uTorrent and LimeWire are open-source software programs available for free on the internet. The uTorrent and LimeWire software allow users to download torrent files that are shared on the BitTorrent network. Torrent files may be referenced by their “infohash”, which uniquely identifies the torrent based on the file(s) associated with the torrent file. Users of the BitTorrent network can find image, video, or other types of files from internet sites such as the Pirate Bay. These types of internet websites provide the torrent files needed to download the desired files from the BitTorrent network. When a user first sets up the P2P client, a folder on the computer is designated to store downloaded files. A file that is downloaded by the user is stored in that designated area until moved or deleted by the user.

9. The BitTorrent network bases all of its file shares on the Secure Hash Algorithm (SHA-1). This mathematical algorithm allows for the digital fingerprinting of data. A torrent file is not the actual digital content, but instead, it defines the files to be shared as a series of contiguous pieces. The SHA-1 hash value for each “piece” of the torrent file is contained within the torrent file, as well as filenames, file sizes and other data. Once you check a file or files with a SHA-1 hashing utility capable of generating this SHA-1 value (the fingerprint), that will be a fixed-length unique identifier for that file or files. The SHA-1 hash is the current Federal Information Processing and Digital Signature Algorithm. The SHA-1 is secure because it is computationally infeasible for two files with different content to have the same SHA-1 hash value.

10. Based on my training, experience, and discussions with other trained law enforcement officers, I know the following facts about the BitTorrent software:

- a. The BitTorrent network is frequently used in the online trading of child pornography. It is used to trade digital files including still images and movie files of child pornography.
- b. During installation of uTorrent or LimeWire requiring the user to provide a “shared” folder, various settings are established that configure the host computer to share—*i.e.*, distribute—files.
- c. Users of the BitTorrent network may receive a selected portion of a torrent file from numerous sources by accepting segments of the file from multiple users and then reassembling the complete file on the local computer.
- d. When a user connects to the BitTorrent network, the user can search for torrent files available for download.

11. Law enforcement has modified the standard software which operates on the BitTorrent network. This law enforcement version only allows the downloading of a single torrent file from a single IP address, as well as the displaying of additional information about the source file and the source user.

12. Law enforcement agencies have compiled databases of known files containing child pornography or child erotica that are checked against files being distributed over P2P networks. For the BitTorrent program used by law enforcement, this list is known as a “Files of Interest” list. The “Files of Interest” list contains files that have been previously viewed by law enforcement officers and determined to contain suspected child pornography or child erotica. Law enforcement also track Files of Interest associated with available torrent files.

## SUMMARY OF PROBABLE CAUSE

### A. Background on the Investigation

13. On or about November 26, 2019, I used a BitTorrent application to conduct an undercover investigation into the internet distribution and possession of child pornography. During this investigation, a device sharing suspected child pornography was located on the BitTorrent files sharing network. I made a direct connection to the device assigned the IP Address 24.126.46.171 (hereinafter "TARGET IP").

14. Once I connected to the TARGET IP, I downloaded files associated with the torrent infohash 971035c84911d6145542e55718a1312a342569ce. The main file folder located within this torrent was named "LS MAGAZINE". I know through my training and experience that the term "LS MAGAZINE" is commonly used to identify images and videos that depict child pornography. I also know through my training and experience that "LS" stands for Lolita Studios. "Lolita" is a commonly search term used by individuals seeking out child pornography on the internet. I reviewed the image files that were downloaded from the TARGET IP and contained in the main file folder: LS MAGAZINE. Through my training and experience, I determined that there were image files contained in this file folder appearing to depict child pornography. The following is a representative sample and description of two image files that I downloaded from the TARGET IP:

a. File Name: ISM-002-069.jpg

SHA1 HASH VALUE: 53E64E59248664840963E37D4701371B6B4DEBCE

File Description: This file depicts three minor females who are all naked. Two of the minor females are holding the third minor female up in the air. The third minor female has her legs spread open to depict a lascivious display of her vagina.

b. File Name: ISM-04-08-022.jpg

SHA1 HASH VALUE: C9717CA010FED499A546AF17BA1F6C4A2D91852E

File Description: This image file depicts two minor females, one prepubescent and one pubescent. Both minor females are standing naked in a bathroom and posed in a manner to depict a lascivious display of their vaginas.

15. I obtained subscriber information from Comcast Communications via legal process. According to Comcast, during the time that I downloaded the child exploitation material as referenced above, the Target IP was assigned to a residential address located in Alexandria, Virginia. Michal Piotrowicz (“PIOTROWICZ”) was the listed subscriber. The listed subscriber’s address was a specific apartment located in the 600 block of Holland Lane in Alexandria.

16. In or about December 2019, I conducted a query via a Department of Homeland Security maintained database. This query revealed that Michal PIOTROWICZ is a lawful permanent resident of the United States and a Citizen of Poland. On an official U.S. Government application signed by PIOTROWICZ on or about October 2019, PIOTROWICZ states that his residential address is the SUBJECT PREMISES as of January 2016.

**B. Search of PIOTROWICZ’s Residence**

17. On or about February 13, 2020, the United States District Court for the Eastern District of Virginia issued a federal warrant to search PIOTROWICZ’s residence in Alexandria, Virginia, for child pornography-related evidence. HSI agents and other law enforcement officers executed the warrant on or about February 21, 2020. PIOTROWICZ was the only person present in the residence at the time of execution, and law enforcement’s search revealed that he lived there alone.

18. During the search, PIOTROWICZ agreed to speak to two law enforcement officers. PIOTROWICZ was advised that he was not under arrest and that he was free to leave. I read PIOTROWICZ his Miranda warnings in the English language after confirming PIOTROWICZ was fluent in the English language. PIOTROWICZ confirmed to law enforcement that he was the only person who lived at the residence and has been living at the residence since January 2016. PIOTROWICZ stated he owned a Dell laptop and a Surface Pro-Tablet. PIOTROWICZ also stated he owned three computer hard drives. PIOTROWICZ provided passwords for his two computer devices and stated he was the only one who used these devices.

19. PIOTROWICZ admitted to using software that operated on the BitTorrent network and that he has been using this software since in or about 2005 or 2006. PIOTROWICZ stated he knew what child pornography was and stated he has downloaded child pornography. PIOTROWICZ stated the first time he had downloaded child pornography was in or about 2012 or 2014. PIOTROWICZ stated although he had downloaded child pornography, he was not targeting underage females; rather, he was targeting images of females who were 20 years old. PIOTROWICZ stated he would search on internet sites such as the Pirate Bay and via the Google internet browser. PIOTROWICZ stated two search terms he has used in the past to find pornography were: Girls/Teenagers and Teenage masturbation.

20. Pursuant to the warrant, law enforcement seized several electronic devices from PIOTROWICZ's residence, including but not limited to, a Dell Precision 5510 laptop.

**C. Forensic Examination of PIOTROWICZ's Devices**

21. Law enforcement personnel then conducted a forensic examination of the electronic devices seized from PIOTROWICZ's residence. The examination uncovered that PIOTROWICZ was using the BitTorrent network to download child pornography. The examination further

uncovered that PIOTROWICZ was using his Dell Precision 5510 laptop to search for, download, and view child pornography.

22. Specifically, the examination of the Dell Precision 5510 laptop revealed that the device has one account under the username "users\Michal". Personal and professional documents belonging to PIOTROWICZ are saved on this device.

23. Contained within the file path: Users\Michal\AppData\Local\Temp\\_tc0\Set 08\ua-08-088.jpg is an image file. This image file was created on February 17, 2020. This file depicts a naked pre-pubescent female lying on a beach towel. The female has no breast development nor pubic hair. The female is posed in a manner to depict a lascivious display of her vagina. A water mark on this image reads: Ukrainian Angels.

24. Contained within the file path: Users\Michal\AppData\Local\Temp\\_tc0\Set 08\ua-08-031.jpg is an image file. This image file was created on February 17, 2020. This file depicts a naked pre-pubescent female standing in thigh-high clear water. The female has no breast development nor pubic hair. The female is posed in a manner to depict a lascivious display of her vagina. A water mark on this image reads: Ukrainian Angels.

25. Contained within the file path: Users\Michal\AppData\Local\Temp\\_tc0\Set 08\ua-08-035.jpg is an image file. This image file was created on February 17, 2020. This file depicts a naked pre-pubescent female sitting on the beach with her ankles crossed. The female has no breast development nor pubic hair. The female is posed in a manner to depict a lascivious display of her vagina. The image also depicts the female pouring sand from her hands into the area of her vagina. A water mark on this image reads: Ukrainian Angels.

26. Contained within the file path: Users\Michal\AppData\Local\Temp\\_tc0\Set 08\ua-08-089.jpg is an image file. This image file was created on February 17, 2020. This file depicts a



naked pre-pubescent female sitting on the beach. The female has no breast development nor pubic hair. The image shows the female's hand on her vagina appearing to simulate masturbation. A water mark on this image reads: Ukrainian Angels.

27. Contained within the file path: Users\Micha\AppData\Local\Temp\\_tc0\Set 08\ua-08-102.jpg is an image file. This image file was created on February 17, 2020. This file depicts a naked pre-pubescent female standing on the beach with a white cloth covering her knees. The female has no breast development nor pubic hair. The female was posed in a manner to depict a lascivious display of her vagina. A water mark on this image reads: Ukrainian Angels.

28. A review of the key word internet searches conducted by the user of the Dell Precision 5510 laptop revealed that the terms "e gold," "angels," "kinder," "kiddy" and "baby j" were all used over 80 times by the user of this device. From my training and experience, I know these terms to be indicative of child pornography.

29. A review of an LNK list on the Dell Precision 5510 laptop revealed numerous titles of files indicative of child pornography. The following files were located within the "F:\downloads" folder. The below files were listed as being viewed in either August 2019 or November 2019. A representative sample of these file names are:

- a. Ls-Magazine 01 (Sweet Twins)\Ism01-01-02.mpg
- b. Ls-Magazine 01 (Sweet Twins)\Ism01-01-02.jpg
- c. Ls-Magazine 01 (Sweet Twins)\Ism01-06-02\_s.jpg
- d. Ls-Magazine 01 (Sweet Twins)\Ism01-09-03.jpg

30. A review of the jump list located on the Dell Precision 5510 laptop revealed numerous titles of files indicative of child pornography. The following files were located within the "F:\downloady" folder on the computer device. A representative sample of these files located in the jump list folder are:

- a. ls-magazine 8 yahre 1yrs! INFANT CAROL-5YO kinderKutje Siterip LS NoLimitsFun kiddy porn.mov
- b. lsh tetitas 9 VIDEO-ANGELS ls-magazine.mpg
- c. LS-Magazine Issue 05 Supple Babies\Videos\lsm05-06-02.avi

31. A review of files recently viewed by the user “Michal” on the Dell Precision 5510 laptop revealed numerous titles of files indicative of child pornography. The following files were marked as recently viewed by the user “Michal”. The following files were listed as being opened from the “F:/downloady” folder on this computer device:

- a. File name: Shining Pretties\_Little Guests, etc (5 sets 3 videos)\v112a.avi  
*This file was accessed on November 27, 2019.*
- b. File name: Desi Indian Amateur Teen with big tits masturbating on webcam.mp4  
*This file was accessed on November 27, 2019.*
- c. File name: Showgirls\_2\_16\_21\_etc (6 sets 1 video)\Lolita Arina-05.avi  
*This file was accessed on January 26, 2020*
- d. File name: LS Stunning Dolls; Little Guests; Star; Touch [6 Sets 3 Videos]\LS-Video 2000 v-47c Lolita.avi  
*This file was accessed on February 15, 2020*

32. A review of internet bookmarks created by the user “Michal” on the Dell Precision 5510 laptop revealed the uTorrent program was used on this device. uTorrent allows users to download torrent files via the internet.

33. The LS-Model series is known to law enforcement as almost always depicting minors under the age of 18 in various provocative poses and or displaying their private parts. The LS-Model series is a series that is highly traded and downloaded by individuals that have a sexual interest in children. As stated previously in this affidavit, on or about November 26, 2019, I

downloaded files from the LS-Model series from an IP address registered to PIOTROWICZ depicting child pornography.

**CONCLUSION**

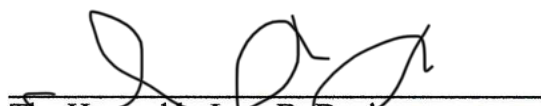
34. For the reasons stated, I respectfully submit that there is probable cause to believe that, between at least in or about November 2019 to on or about February 17, 2020, in the Eastern District of MICHAL JERZY PIOTROWICZ knowingly received child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b)(1). Therefore, I respectfully request that a criminal complaint and arrest warrant be issued for PIOTROWICZ.

Respectfully submitted,



Special Agent  
Raymond Abruzzese  
Homeland Security Investigations

Respectfully submitted and attested to in accordance with  
the requirements of Fed. R. Crim. P. 4.1 via telephone on July 17, 2020.

  
The Honorable Ivan D. Davis  
United States Magistrate Judge